

INFORMATION RECORDING DEVICE AND INFORMATION RECORDING AND REPRODUCING DEVICE

Publication number: JP2003115830

Publication date: 2003-04-18

Inventor: SHINDO TOMOYUKI; OISHI TAKESHI

Applicant: VICTOR COMPANY OF JAPAN

Classification:

- **international:** G06F12/14; G06F21/00; G06F21/24; G11B20/00; G11B20/10; H04L9/06; H04L9/16; H04N5/76; H04N5/91; H04N5/913; H04N5/781; H04N5/804; G06F12/14; G06F21/00; G11B20/00; G11B20/10; H04L9/06; H04L9/14; H04N5/76; H04N5/91; H04N5/913; H04N5/781; H04N9/804; (IPC-7): H04L9/06; G06F12/14; G11B20/10; H04L9/16; H04N5/76; H04N5/91

- european: G06F21/00N9A1; G11B20/00P; H04N5/913

Application number: JP20010307160 20011003

Priority number(s): JP20010307160 20011003

Also published as:



EP1300843 (A2)



US2003065925 (A1)

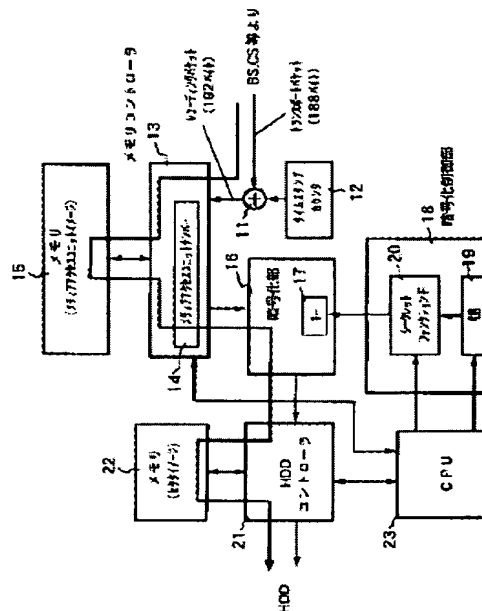


EP1300843 (A3)

Report a data error here

Abstract of JP2003115830

PROBLEM TO BE SOLVED: To solve a problem that the load of a device is made extremely heavy since complicated processing is required when a block to be enciphered by the same cryptographic key is made short and that operation is made difficult since it is necessary to manage how many data blocks of prescribed units are skipped or the like in high speed reproducing. **SOLUTION:** A recording packet from a memory 15 is read out for the unit of a media access unit and supplied to an enciphering part 16 after assigning a media access unit number 14 and under control from an encipher control part 18, block enciphering is performed by a memory controller 13. A class 19, which is a base for common key stream generation, to become the source of the cryptographic key is written from a CPU or the like to the encipher control part 18. On the basis of the class 19 and the media access unit number 14, the encipher control part 18 generates a secret function F 20 and calculates a cryptographic key 17 by using this function. The data from the memory 15 are enciphered based on the cryptographic key 17 and stored on an HDD by the enciphering part 16.



Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-115830

(P2003-115830A)

(43)公開日 平成15年4月18日(2003.4.18)

(51)Int.Cl. ⁷	識別記号	FI	キーワード(参考)
H04L 9/06		G06F 12/14	320B 5B017
G06F 12/14	320	G11B 20/10	H 5C052
G11B 20/10			311 5C053
	311	H04N 5/76	Z 5D044
H04L 9/16		H04L 9/00	611A 5J104

審査請求 未請求 請求項の数18 ○L (全 10 頁) 最終頁に続く

(21)出願番号 特願2001-307160(P2001-307160)

(22)出願日 平成13年10月3日(2001.10.3)

(71)出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72)発明者 進藤 朋行

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(72)発明者 大石 剛士

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(74)代理人 100085235

弁理士 松浦 兼行

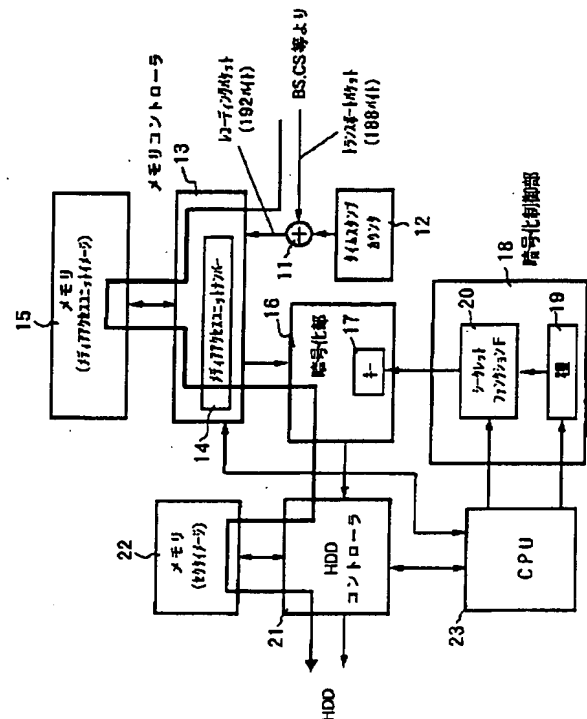
最終頁に続く

(54)【発明の名称】 情報記録装置及び情報記録再生装置

(57)【要約】

【課題】 同一の暗号鍵で暗号化される区間を短くすると、複雑な処理が必要になり、装置における負担が非常に重くなる。また、高速再生では、いくつかの所定単位の水タ区間を飛ばしたか等を管理する必要があり、運用が困難である。

【解決手段】 メモリコントローラ13は、メモリ15からのレコーディング packets を、メディアアクセスユニット単位で読み出して、メディアアクセスユニットナンバー14を割り当てて暗号化部16に供給して、暗号化制御部18からの制御の下にブロック暗号化を行う。CPU等から暗号鍵の元になる、共通の鍵系列発生用基数である種19を暗号化制御部18に書き込む。暗号化制御部18は、種19とメディアアクセスユニットナンバー14とに基づいてシークレットファンクションF20を生成し、これを用いて暗号鍵17を算出する。暗号化部16はメモリ15からのデータを、暗号鍵17に基づいて暗号化してHDDに記憶する。



【特許請求の範囲】

【請求項 1】 記録すべき情報を所定のデータ量毎に分割すると共に、前記所定のデータ量単位のそれぞれに連続的に変化する連続番号を割り当てる連続番号付与手段と、

一つのライセンスで管理される範囲毎において共通の鍵系列発生用基数が設定され、この鍵系列発生用基数と所定のデータ量毎に変化する番号とに基づき生成される秘密に定義される関数から暗号鍵を生成する暗号化制御手段と、

前記連続番号と前記所定のデータ量単位内の各データが記録される先頭の論理アドレスとを関連付けて別の情報として格納する格納手段と、

前記記録すべき情報を、前記所定のデータ量よりも小さいデータ量の最小分割単位毎に、前記暗号化制御手段からの前記暗号鍵に基づきブロック暗号化を行う暗号化手段と、

前記暗号化手段により暗号化された信号を前記記録媒体に記録すると共に、前記格納手段に格納された前記別の情報を記録する記録手段とを有し、前記暗号鍵を前記所定のデータ量毎に更新して暗号化を行うことを特徴とする情報記録装置。

【請求項 2】 前記暗号化制御手段は、前記鍵系列生成用基数と前記連続番号とに基づき生成される秘密に定義される関数から暗号鍵を生成することを特徴とする請求項 1 記載の情報記録装置。

【請求項 3】 前記暗号化制御手段は、前記鍵系列生成用基数と前記先頭の論理アドレスを利用した番号とに基づき生成される秘密に定義される関数から暗号鍵を生成することを特徴とする請求項 1 記載の情報記録装置。

【請求項 4】 前記暗号化手段は、MPEG2 トラnsポートパケットに 4 バイトのソースパケットヘッダを付加した 192 バイトを、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行うことを特徴とする請求項 1 記載の情報記録装置。

【請求項 5】 前記暗号化手段は、MPEG2 トラnsポートパケットに 4 バイトのソースパケットヘッダを付加した 192 バイトのうち、前記ソースパケットヘッダと MPEG2 トラnsポートパケットの先頭の 4 バイトのヘッダとを除外した 184 バイトを、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行うことを特徴とする請求項 1 記載の情報記録装置。

【請求項 6】 前記暗号化手段は、前記記録媒体の論理セクタと同じビット数の前記情報を、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行うことを特徴とする請求項 1 記載の情報記録装置。

【請求項 7】 前記暗号化手段は、前記最小分割単位の一部を前記暗号鍵に基づきブロック暗号化を行った暗号部分とし、かつ、前記最小分割単位の残りを暗号化しない非暗号部分とし、同一の前記所定のデータ量中で特定

の最小分割単位群だけを同一の暗号鍵で暗号化すると共に、前記非暗号部分中のビットにより暗号化したか否かを示すことを特徴とする請求項 1 記載の情報記録装置。

【請求項 8】 前記暗号化手段は、前記所定のデータ量単位を構成する複数の前記最小分割単位のうち、各データ量単位の先頭より特定のルールに則って一部の最小分割単位のみを暗号化し、それ以外の最小分割単位は暗号化しないことを特徴とする請求項 1 記載の情報記録装置。

10 【請求項 9】 前記暗号化制御手段は、前記暗号化手段が同一の暗号鍵を使用する範囲と前記暗号鍵とを、前記所定のデータ量単位毎に付与される前記連続番号と関連付けて、前記暗号鍵を生成することを特徴とする請求項 1 記載の情報記録装置。

【請求項 10】 記録すべき情報を所定のデータ量毎に分割すると共に、前記所定のデータ量単位のそれぞれに連続的に変化する連続番号を割り当てる連続番号付与手段と、

一つのライセンスで管理される範囲毎において共通の鍵系列発生用基数が設定され、この鍵系列発生用基数と前記所定のデータ量毎に変化する番号とに基づき生成される秘密に定義される関数から暗号鍵を生成する暗号化制御手段と、

前記連続番号と、前記所定のデータ量単位内の各データが記録される先頭の論理アドレスとを関連付けて別の情報として格納する格納手段と、

前記記録すべき情報を、前記所定のデータ量よりも小さいデータ量の最小分割単位毎に、前記暗号化制御手段からの前記暗号鍵に基づきブロック暗号化を行う暗号化手段と、

前記暗号化手段により暗号化された信号を前記記録媒体に記録すると共に、前記格納手段に格納された前記別の情報を記録し、記録した信号を再生する記録再生手段と、

前記共通の鍵系列発生用基数が設定され、この鍵系列発生用基数と前記記録媒体から再生された信号から取得した前記所定のデータ量毎に変化する番号とに基づき生成される秘密に定義される関数から復号鍵を生成する復号化制御手段と、

40 前記記録再生手段により前記記録媒体から再生された信号を、前記復号化制御手段からの前記復号鍵を使用して前記最小分割単位毎に復号化する復号化手段とを有し、前記暗号鍵又は前記復号鍵を前記所定のデータ量毎に更新して暗号化又は復号化を行うことを特徴とする情報記録再生装置。

【請求項 11】 前記暗号化制御手段は、前記鍵系列生成用基数と前記連続番号とに基づき生成される秘密に定義される関数から暗号鍵を生成することを特徴とする請求項 10 記載の情報記録再生装置。

50 【請求項 12】 前記暗号化制御手段は、前記鍵系列生

成用基数と前記先頭の論理アドレスを利用した番号とに基づき生成される秘密に定義される関数から暗号鍵を生成することを特徴とする請求項 10 記載の情報記録再生装置。

【請求項 13】 前記暗号化手段は、MPEG2 トラnsポートパケットに 4 バイトのソースパケットヘッダを付加した 192 バイトを、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行うことを特徴とする請求項 10 記載の情報記録再生装置。

【請求項 14】 前記暗号化手段は、MPEG2 トラnsポートパケットに 4 バイトのソースパケットヘッダを付加した 192 バイトのうち、前記ソースパケットヘッダと MPEG2 トラnsポートパケットの先頭の 4 バイトのヘッダとを除外した 184 バイトを、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行い、前記復号化手段は、前記 MPEG2 トラnsポートパケットに 4 バイトのソースパケットヘッダを付加した 192 バイトのうち、前記ソースパケットヘッダと MPEG2 トラnsポートパケットの先頭の 4 バイトのヘッダとを除外した 184 バイトを、前記最小分割単位として前記復号鍵に基づきブロック復号化を行うことを特徴とする請求項 10 記載の情報記録再生装置。

【請求項 15】 前記暗号化手段は、前記記録媒体の論理セクタと同じビット数の前記情報を、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行い、前記復号化手段は、前記記録媒体の論理セクタと同じビット数の前記記録媒体の再生信号を、前記最小分割単位として前記復号鍵に基づきブロック復号化を行うことを特徴とする請求項 10 記載の情報記録再生装置。

【請求項 16】 前記暗号化手段は、前記記録媒体の論理セクタと同じビット数の前記情報を、前記最小分割単位として前記暗号鍵に基づきブロック暗号化を行い、前記記録媒体の再生信号の該記録媒体の論理セクタと同じビット数を、前記最小分割単位として前記復号鍵に基づきブロック復号化を行うことを特徴とする請求項 10 記載の情報記録再生装置。

【請求項 17】 前記暗号化手段は、前記最小分割単位の一部を前記暗号鍵に基づきブロック暗号化を行った暗号部分とし、かつ、前記最小分割単位の残りを暗号化しない非暗号部分とし、同一の前記所定のデータ量中で特定の最小分割単位群だけを同一の暗号鍵で暗号化すると共に、前記非暗号部分中のビットにより暗号化したか否かを示し、前記復号化手段は、再生信号中の前記非暗号部分中のビットが暗号化を示しているときに前記最小分割単位の一部を復号鍵で復号化することを特徴とする請求項 10 記載情報記録再生装置。

【請求項 18】 前記暗号化制御手段は、前記暗号化手段が同一の暗号鍵を使用する範囲と前記暗号鍵とを、前記所定のデータ量単位毎に付与される前記連続番号と関連付けて、前記暗号鍵を生成し、前記復号化制御手段

は、前記復号化手段が同一の復号鍵を使用する範囲と前記復号鍵とを、前記所定のデータ量単位毎に付与される前記連続番号と関連付けて、前記復号鍵を生成することを特徴とする請求項 10 記載の情報記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は情報記録装置及び情報記録再生装置に係り、特に情報を暗号化して記録媒体に記録する情報記録装置及び情報記録再生装置に関する。

【0002】

【従来の技術】従来より、通信の分野において、高速の暗号化や復号化が要求される場合の暗号方式として、共有鍵暗号方式が知られている。この暗号方式は、暗号化に用いられる鍵（暗号鍵）と復号化に用いられる鍵（復号鍵）が同一であるという特徴がある。暗号化する装置は暗号鍵を復号化する装置に知らせる必要があるため、鍵を共有するための手段が各種提案されているが、いずれも基本的に安全に鍵を共有するには複雑な手法を必要とする。

【0003】この共有鍵暗号方式を、画像及び音声データ（以下、AVデータ、あるいはコンテンツともいう）を記録再生する装置に適用した場合、一般にAVデータのデータ量が大きく、これを一個の暗号鍵で暗号化して記録媒体に記録しても、暗号鍵が露見した場合は、AVデータがすべて復号化できてしまう（一つの映画コンテンツを一個の暗号鍵で暗号化して記録した場合、まるまる復号化されてしまう）。

【0004】そこで、AVデータを暗号化するための鍵が露見した場合でもその被害をできるだけ少なくするためには、AVデータをあるデータ量毎に区切って暗号化するブロック暗号が考えられる。このブロック暗号では、一般的に高速の暗号化や復号化が要求される場合、その処理速度と回路規模の問題から 64 ビット程度のブロック暗号が利用されることが多いが、この程度の暗号は今後のプロセッサ等の進化を考えると、早晚一定の期間内に解読されてしまう可能性が否定できない。従って、同一の暗号鍵で暗号化される区間（データ長）はできるだけ短い方がアタックに対して強くなる。

【0005】

【発明が解決しようとする課題】しかるに、暗号化される区間を短くすると、その区間毎に暗号鍵をどのように更新していくかが問題となる。AVデータ暗号化のための鍵をそのまま保存することはできないので、別の強力な暗号（通常、公開鍵暗号が用いられることが多い）で暗号化されて保存されるが、暗号鍵の個数が多いとAVデータを暗号化するための暗号鍵を更に暗号化して保存するための複雑な処理が必要になり、装置における負担が非常に重くなる。また、暗号鍵の数も飛躍的に増えてしまい、その分、AVデータの記録時間が失われてしま

う。

【0006】また、上記の問題を解決するために、伝送する暗号鍵を1個とし、2回目からは共通の方法で暗号鍵、復号鍵を変更していくことが考えられるが、その場合、AVデータの途中から再生する場合に復号できない（必ず、最初から復号していかないと成り立たない）ことが考えられる。

【0007】一方、情報記録再生装置では、通常再生だけではなく高速再生などの特殊再生も行えることが望ましいが、高速再生では、記録媒体上の記録AVデータは、高速再生のための補助データを用いて当初記録した順番とは異なって、飛び飛びに再生することが行われる。その高速再生の際に、AVデータの所定単位毎に新たな復号化のための鍵を算出することや、記録時にAVデータの所定単位毎に暗号化／復号化のための鍵を公開鍵暗号の技術を用いて暗号化／復号化する演算は膨大なプロセッサの負荷となる。

【0008】従って、できるだけ細かな単位毎にAVデータ（コンテンツ）の暗号化を切り替えると共に、コンテンツの暗号化／復号化のための鍵を暗号化／復号化する公開鍵暗号の演算回数を少なくするための方法として、コンテンツ（又はセッション）毎に1回公開鍵暗号の技術を用いて、コンテンツ暗号化／復号化のための鍵の種となる情報を暗号化／復号化して、実際のコンテンツの暗号化／復号化のための鍵は、その種の情報より秘密に決定されている関数を用いて順次算出し、その鍵の交代のタイミングを1ビットの情報（オッドキー／イーブンキーのいずれを用いるかの指示）を用いて逐次制御する方法がある。

【0009】この方法では、順次交代（ここで交代といっているのは、2つだけの鍵をただ単に交代して使っているのではなく、オッド1、イーブン1、オッド2、イーブン2、・・・といった具合に、オッドキーとイーブンキーとを交代しながら、更にその内容も順次更新されていくものである。）される鍵を公開鍵暗号で保護されるコンテンツ暗号化のための種から順次所定の演算（例えば、秘密に定義した関数F（種＋交代回数）など）で生成する方法がある。これは、公開鍵暗号で保護される初期値等を出発点に順次オッド／イーブンのキーが交代する毎に初期値からカウントアップを行い、その結果に対して一方向関数等の処理を施した結果の規約で定めた一部をコンテンツ暗号化／復号化のための鍵として利用する方法である。

【0010】しかし、この方法では、連続してコンテンツを扱うような場合、例えば通常記録／通常再生を行う場合やデジタルインタフェースにてコンテンツのAVデータを伝送する場合には特に問題ないが、高速再生を行うために連続して記録された内容の所々をスキップしながら再生を行うような場合、次に使用されるべきAVデータの暗号化／復号化のための暗号鍵算出のため、い

くつの所定単位 of データ区間を飛ばしたか等を管理する必要があり、運用が困難である。

【0011】本発明は以上の点に鑑みなされたもので、できるだけ細かな単位毎にAVデータ（コンテンツ）の暗号化を切り替えることにより、暗号鍵が露見した場合でも、その被害を少なくし得る情報記録装置及び情報記録再生装置を提供することを目的とする。

【0012】また、本発明の他の目的は、多くの暗号鍵を用いて、処理の負担少なくAVデータを暗号化して記録し得る情報記録装置及び情報記録再生装置を提供することにある。

【0013】更に、本発明の他の目的は、高速再生時も暗号化したデータを再生して容易に復号し得る情報記録再生装置を提供することにある。

【0014】また、本発明の更に他の目的は、一つの記録媒体上に複数のコンテンツが最小単位毎にマルチプレクスされた状態で記録されるような場合、暗号化したいコンテンツのみを選択的に暗号化し得る情報記録装置及び情報記録再生装置を提供することにある。

【0015】

【課題を解決するための手段】上記の目的を達成するため、本発明の情報記録装置は、記録すべき情報を所定のデータ量毎に分割すると共に、所定のデータ量単位のそれぞれに連続的に変化する連続番号を付与する連続番号付与手段と、一つのライセンスで管理される範囲毎において共通の鍵系列発生用基数が設定され、この鍵系列発生用基数と所定のデータ量毎に変化する番号とに基づき生成される秘密に定義される関数から暗号鍵を生成する暗号化制御手段と、連続番号と、所定のデータ量単位内の各データが記録される先頭の論理アドレスとを関連付けて別の情報として格納する格納手段と、記録すべき情報を所定のデータ量よりも小さいデータ量の最小分割単位毎に、暗号化制御手段からの暗号鍵に基づきブロック暗号化を行う暗号化手段と、暗号化手段により暗号化された信号を記録媒体に記録すると共に、格納手段に格納された別の情報を記録する記録手段とを有する構成としたものである。

【0016】この発明では、記録すべき情報を暗号化するための暗号鍵を所定のデータ量毎に更新しているため、暗号鍵が露見した場合でも、その被害を最小限に止めることができる。

【0017】ここで、上記の連続番号付与手段は、一連のレコードの先頭より所定のデータ量単位に分割した各々の単位に、先頭より連続して付与される番号を連続番号として付与するか、又は一連のレコードの先頭より所定のデータ量単位に分割した各々の単位に対応して、格納手段に格納される先頭の論理アドレスを利用して連続番号として付与することを特徴とする。

【0018】また、本発明の上記の暗号化手段は、MP EG2トランスポートパケットに4バイトのソースパケ

ットヘッダを付加した192バイトを、最小分割単位として暗号鍵に基づきブロック暗号化を行うか、MPEG2トランスポートパケットに4バイトのソースパケットヘッダを付加した192バイトのうち、ソースパケットヘッダとMPEG2トランスポートパケットの先頭の4バイトのヘッダとを除外した184バイトを、最小分割単位として暗号鍵に基づきブロック暗号化を行うか、又は記録媒体の論理セクタと同じビット数の情報を、最小分割単位として暗号鍵に基づきブロック暗号化を行うことを特徴とする。

【0019】また、本発明は上記の目的を達成するため、上記の暗号化手段を、最小分割単位の一部を暗号鍵に基づきブロック暗号化を行った暗号部分とし、かつ、最小分割単位の残りを暗号化しない非暗号部分とし、同一の所定のデータ量中で特定の最小分割単位群だけを同一の暗号鍵で暗号化すると共に、非暗号部分中のビットにより暗号化したか否かを示すことを特徴とする。

【0020】この発明では、一つの記録媒体上に複数の情報（コンテンツ）が所定のデータ量単位毎にマルチプレクスされた状態で記録されるような場合、暗号化した情報のみを暗号化することができる。

【0021】また、上記の目的を達成するため、本発明は上記の暗号化手段を、所定のデータ量単位を構成する複数の最小分割単位のうち、各データ量単位の先頭より特定のルールに則って一部の最小分割単位のみを暗号化し、それ以外の最小分割単位は暗号化しないようにしたことを特徴とする。

【0022】この発明では、一つの記録媒体上に複数の情報（コンテンツ）が所定のデータ量単位毎にマルチプレクスされた状態で記録されるような場合、情報毎の種別を示すIDの最小分割単位は暗号化せず、ID毎に適用する暗号鍵の系列を異なるものにすることができる。

【0023】また、上記の目的を達成するため、本発明は上記の暗号化制御手段を、暗号化手段が同一の暗号鍵を使用する範囲と暗号鍵とを、所定のデータ量単位毎に付与される連続番号と関連付けて、暗号鍵を生成することを特徴とする。

【0024】また、上記の目的を達成するため、本発明の情報記録再生装置は、上記の本発明の情報記録装置の記録系に加えて、更に、暗号化手段により暗号化された信号を、連続番号と記録媒体のアクセスする先頭の論理アドレスとをそれぞれ関連付けて記録媒体に記録し、記録した信号を再生する記録再生手段と、共通の鍵系列発生用基数が設定され、この鍵系列発生用基数と記録媒体から再生された信号から取得した所定のデータ量毎に変化する番号とに基づき生成される秘密に定義される関数から復号鍵を生成する復号化制御手段と、記録再生手段により記録媒体から再生された信号を、復号化制御手段からの復号鍵を使用して最小分割単位毎に復号化する復号化手段とを有する構成としたものである。

【0025】この発明では、記録媒体上に暗号化されて記録されているデータの一部分を飛び飛びで再生する高速再生時でも、次にアクセスする所定のデータ量単位の連続番号と論理アドレスの対照表を参照することで、迅速に復号のための鍵を算出することができる。

【0026】

【発明の実施の形態】次に、本発明の実施の形態について図面と共に説明する。図1は本発明になる情報記録装置及び情報記録再生装置の要部の一実施の形態のブロック図を示す。この実施の形態は、AVデータを記録媒体としてハードディスク（以下、HDDともいう）に記録し、再生する装置である。

【0027】AVデータのような高速な転送レートが要求されるデータをHDD等の記録媒体に記録・再生する場合には、所定のデータ量（記録媒体の容量やコントローラLSIのバッファメモリ量等の様々な要因で決定されるもの）毎に連続的なLBA（論理ブロックアドレス）に記録するような構成をとる。これは、連続するデータがセクタ（例えば、標準的なHDDでは512Bなど）毎に離れた領域に書き込まれると、データを読み出したり書き込んだりする時間に比較して、データを記録再生するための位置にヘッドを移動するための時間（通常、シーク時間という）が多くなり、実効的な記録再生の速度が著しく低下することになる現象を避けるために行われる。通常は、この単位が約1MBとか2MBといったサイズが選択される。

【0028】一方、現行のBSデジタル放送やCSデジタル放送からのデータをHDDに記録する場合には、MPEG2（Moving Picture Experts Group 2）のトランスポートストリーム（TS）のままタイムスタンプを付加してHDDに記録していく方法がある。これは、テープ媒体においてはD-VHS（登録商標）規格の磁気記録再生装置等で実現されている方法で、放送で送られたデータをそのまま記録媒体上に記録することができ、外部から入力された信号を記録したり、記録済みの信号を外部にデジタル出力したりする時の変換操作を軽くすることができるといったメリットがある。

【0029】これらを前提に図1の実施の形態の情報記録装置及び情報記録再生装置は以下の処理を行う。BSデジタル放送又はCSデジタル放送等を受信して得られたMPEG2規定の188バイト固定長のトランスポートパケットは加算器11に供給され、ここでそのトランスポートパケットのシステムクロックに同期したタイムスタンプカウンタ12からの、トランスポートパケットの到着時刻に対応した4ビットの値がタイムスタンプとして加算される。

【0030】これにより、加算器11からは図2（A）に31で示す最小分割単位である188バイトのトランスポートパケットに、同図（A）に32で示す4バイトのタイムスタンプがソースパケットヘッダとして付加さ

れた合計 192 バイトのレコーディングパケットが取り出され、メモリコントローラ 13 に供給される。

【0031】上記の 4 バイトのソースパケットヘッダ 32 は、図 2 (B) にバイト単位で示すように、33a と 33b で示す下位 9 ビットが、27MHz のシステムクロックを単位として 0 から 299 までの値をとるレコーディングタイムスタンプエクステンションで、34a、34b 及び 34c で示す下位 10 ビット目から 28 ビット目までの 19 ビットが、エクステンションが 299 から 0 に変わる時に +1 されるレコーディングタイムスタンプベースであり、残りの上位 4 ビット 35 が予約とされたフォーマットである。

【0032】レコーディングタイムスタンプエクステンションの MSB はソースパケットヘッダの上位 24 ビット目 (33b) に配置され、LSB は下位 1 ビット目に配置される。また、レコーディングタイムスタンプベースの上位 4 ビットはソースパケットヘッダの上位 5 ビット目から 8 ビット目 (34c) に配置される。メモリコントローラ 13 は、加算器 11 からのレコーディングパケットを入力として受け、メモリ 15 に格納する。

【0033】ここで、通常、HDD のセクタサイズは 512 バイト (B) で構成される。この中に上記のレコーディングパケットを効率良くマッピングするために、この実施の形態では、図 3 に示すように、3 つのセクタを単位とし、1 番目のセクタ N には、192 バイトのレコーディングパケット 41 及び 42 と、一つのレコーディングパケットの 2/3 の 128 バイト分のパケット 43a とが配置され、2 番目のセクタ N+1 には、残りの 1/3 の 64 バイト分 43b と、続く 2 つのレコーディングパケット 44、45 と、次の一つのレコーディングパケットの 1/3 の 64 バイト分 46a とが配置され、3 番目のセクタ N+2 には、残りの 2/3 の 128 バイト分 46b と、続く 2 つのレコーディングパケット 47 及び 48 とが配置されている。

【0034】すなわち、メモリコントローラ 13 は、連続する 3 つのセクタ単位で 7 つのレコーディングパケットが配置されるように、メモリ 15 にレコーディングパケットを記憶する。この明細書では、図 3 に示した連続した 3 つのセクタで構成される単位をミニマムアクセスユニット (Minimum Access Unit) と定義する。なお、セクタには図示しないが、0 から始まる論理アドレスが割り振られている。

【0035】図 4 はセクタサイズが 512 B である HDD との整合性を考慮した値として 3 セクタ分 1536 B (= 512 B × 3) からなるミニマムアクセスユニットを示す。また、図 5 は 1 セクタが 2048 B から構成される光ディスクなどを考慮した、3 セクタ分 6144 B (= 2048 B × 3) からなるミニマムアクセスユニットを示す。この値は、HDD との共用も同時に実現している。

【0036】また、図 6 に示す上記のミニマムアクセスユニットの複数 N 個からなる構成は、AV オブジェクトユニット (AV Object Unit) を構成する。また、この AV オブジェクトユニットは、複数のミニマムアクセスユニットから構成され、同時に GOP と呼ばれる MPEG 方式により圧縮された画像の単位から構成されている。なお、MPEG では、GOP と呼ばれる単位の先頭からデコーディングを開始できるような設定ができる。

【0037】一方、HDD にどのように AV データを記録/再生するか考慮した場合、連続する記録領域が細かく、離れた場所に配置されると、必要な箇所をシークするための時間が実際の記録再生を行う時間に対して支配的となり、実効的な転送速度が確保できなくなってしまう。AV データは、一般的に非常に膨大なデータ量となるため、連続する LBA (論理ブロックアドレス) に記録されるデータ量を比較的多く (例えば、1.5MB など) とっても特段問題なく、逆にディスク上の細かなフラグメンテーションが発生しなくなるため、実効的な転送速度を確保しやすい。

【0038】そこで、本実施の形態では、図 7 に示すように、通常、複数の AV オブジェクトユニットを含む単位をメディアアクセスユニット (Media Access Unit) と定義して、このメディアアクセスユニット単位で HDD に対して記録再生を行う。なお、メディアアクセスユニットは、例えば 1.5MB であり、図 7 に点線を付して示すように、メディアアクセスユニットと AV オブジェクトユニットの切れ目は必ずしも同一ではない。

【0039】再び図 1 に戻って説明するに、メモリコントローラ 13 は、メモリ 15 に格納されている前記レコーディングパケットを、前記メディアアクセスユニット単位で読み出して、連続的な番号であるメディアアクセスユニットナンバー 14 を割り当てて暗号化部 16 に供給して、暗号化制御部 18 からの制御の下に例えばレコーディングパケット単位毎にブロック暗号化を行う。なお、メディアアクセスユニットナンバー 14 は暗号化しない。

【0040】ここで、高速でデータを暗号化又は復号化する場合、一般的にはデータそのものを暗号化/復号化するための暗号化/復号化手段と、データ暗号化/復号化のための鍵を保護するために鍵暗号化/復号化手段が用いられることが多い。この場合、高速でデータを暗号化/復号化するための手段として回路化が容易なブロック共通鍵暗号 (例えば、DES など) を用い、暗号化/復号化のための鍵を強力に保護するために RSA や楕円曲線暗号などの公開鍵暗号を用いる。これは、一般に公開鍵暗号は強度が高いが、大量のデータ量を扱うには演算量が多すぎるため、この両者の長所を組み合わせた方法を用いるためである。

【0041】次に、コンテンツの暗号化/復号化の手段であるが、一般に回路規模が大きくなるために、暗

号鍵は56ビットや64ビット、長くても128ビット程度であり、暗号鍵を推定される危険性が否定できない。また、暗号鍵は数学的演算によって解析される以外に様々な脅威にさらされている。例えば、設計にかかわった人間から漏洩する場合も考えられる。

【0042】このような場合、コンテンツを暗号化／復号化するための鍵がコンテンツ全体に有効なものでなく、コンテンツのごく限られた一部期間のみ有効なもので、順次変化していくとすると、不正に暗号を解読しようと試みる者の氣勢をそぐことができる。その一つの方法として、先に定義したメディアアクセスユニット毎にコンテンツの暗号化／復号化のための鍵を更新する方法が考えられる。

【0043】一方、HDDに記録したデータを高速再生する場合、高速再生のための補助データを用いて当初記録した順番とは異なって、記録データは飛び飛びに再生されるが、その際にメディアアクセスユニット毎に新たな復号化のための鍵を算出することや、記録時にメディアアクセスユニット毎に（この実施の形態では、メディアアクセスユニットは1.5MBとしているので、記録時のデータレートが例えば8Mbpsであるとする、約1.5秒毎に、記録時のデータレートが24Mbpsであるとする、約0.5秒分毎に）、コンテンツの暗号化／復号化のための鍵を公開鍵暗号の技術を用いて暗号化／復号化する演算は膨大なプロセッサの負荷となる。

【0044】従って、できるだけ細かな単位毎にコンテンツの暗号化を切り替えると共に、コンテンツの暗号化／復号化のための鍵を暗号化／復号化する公開鍵暗号の演算回数を少なくしてプロセッサの負荷を軽減するために、前述したコンテンツ暗号化／復号化のための鍵を、その種の情報より秘密に決定されている関数を用いて順次算出し、その鍵の交代のタイミングを1ビットの情報を用いて逐次制御する方法が考えられるが、前述したように、高速再生時には次に使用されるべきコンテンツ暗号化／復号化のための暗号鍵算出のため、幾つのメディアアクセスユニット（ここでは、メディアアクセスユニット単位でコンテンツ暗号化／復号化のための鍵を更新していると仮定）を飛ばしたか等を管理する必要がある、運用が困難である。

【0045】そこで、この実施の形態では、メディアアクセスユニット毎に付与されるメディアアクセスユニットナンバー14（又は先頭のメディアアクセスユニットからの通し番号）と関連付けられたコンテンツ暗号化／復号化のための鍵算出を行うことで、次にアクセスするメディアアクセスユニットのメディアアクセスユニットナンバー14から一意に復号のための鍵を算出することができるようにしたものである。

【0046】すなわち、図1において、中央処理装置（CPU）23は暗号鍵の基になる、共通の鍵系列発生用基数である種（SEED）19を暗号化制御部18に書き

込むと共に、メモリコントローラ13に供給するメディアアクセスユニットナンバー14と同じメディアアクセスユニットナンバーを暗号化制御部18に供給する。暗号化制御部18は、この種19とCPU23からのメディアアクセスユニットナンバーとに基づいて秘密に定義した関数（シークレットファンクション）F20を生成し、これを用いて暗号鍵17を算出して暗号化部16に供給する。

【0047】暗号化部16はメモリコントローラ13によりメモリ15からメディアアクセスユニット単位で読み出され、連続的な番号であるメディアアクセスユニットナンバー14が付加されたデータを、上記の暗号鍵17に基づいて例えばレコーディングパケット単位でブロック暗号化する。暗号化部16で暗号化されたデータは、HDDコントローラ21によりメモリ22に一旦格納された後、読み出されてHDDに書き込まれる。

【0048】ここで、ハードディスクや光ディスク等はアクセスできる最小単位としてセクタという概念が存在し、セクタには識別用の数字、すなわち論理アドレスが割り振られている。この実施の形態では、メディアアクセスユニットを記録する際にメディアアクセスユニットナンバー14とハードディスクの論理アドレスとが関連付けられて記録される。すなわち、CPU23は上記のメディアアクセスユニットナンバー14と、HDDに記録するメディアアクセスユニットナンバー14内のデータの先頭の論理アドレスとを関連付けてCPU23内のメモリにテーブルとして格納する。

【0049】つまり、同じ値のメディアアクセスユニットナンバー14が付与される複数のセクタ（一連のレコードの先頭より所定のデータ量単位に分割したそれぞれの単位）の先頭の論理アドレスと、メディアアクセスユニットナンバー14とが上記のテーブルに格納される。

【0050】このテーブルが高速再生を行うための補助情報として別ファイルに整理格納される。そして、メディアアクセスユニットナンバーのN番目のデータはHDDの論理アドレスMに記録するという情報をコンテンツ（AVデータ）とは別の情報（ファイル）としてHDDに記録する。また、種19はCPU等が公開鍵等の強力な暗号手段を用いてHDDにAVデータとは別途記録する。

【0051】このように、この実施の形態では、メディアアクセスユニットナンバー14と種19とから暗号鍵を算出するようにしているので、記録時に容易に順次必要となるコンテンツ暗号化のための鍵17を算出することができる。

【0052】上記のシークレットファンクションF20としては、例えば、SHA (SecureHash Algorithm)-1などの一方向関数を施した結果を利用することができる。また、その他にもDES等のブロック暗号の手順を利用して、メディアアクセスユニットナンバー14を入

カベクタに、種19を暗号鍵としてDESの演算結果を利用することができる。上記方法に関しては、これらの値をそのまま利用することも定数倍や特定のビット抽出、ビットシフト、論理和や論理積の演算等を組み合わせて利用することも可能である。

【0053】すなわち、本実施の形態は、メディアアクセスユニット単位で変更される鍵（キー）17は、一つのライセンスで管理される範囲毎において、共通の鍵系列発生用基数を持ち、この基数と予め関数の一部に上記のメディアアクセスユニット毎に与えられるメディアアクセスユニットナンバーが含まれる鍵生成用関数であるシークレットファンクション20から、個別のメディアアクセスユニット単位毎の暗号鍵を生成するものである。

【0054】コンテンツ暗号化／復号化の方法として、例えばDESのCBC（Cipher Block Chaining）モードを利用することが考えられる。CBCモードを利用する理由としては、再帰的な暗号化がなされるので、単純な暗号化の演算よりも内容の類推が行いにくいなどのメリットがあるためである。また、CBCモードの初期化を行う単位としてはDESが64ビット単位の演算を行う必要性と対応して、8バイトの倍数である必要がある。

【0055】なお、上記の実施の形態では、暗号化／復号化は192Bのレコーディングパケット単位で行うように説明したが、本発明はこれに限定されるものではなく、例えば4バイトのソースパケットヘッダとMPEGのトランスポートストリームの先頭4バイトのヘッダを除外した184バイト単位で行う方法、512BのHDDセクタ単位で行う方法、2048バイト単位の光ディスクのセクタ単位で行う方法でもよい。

【0056】192B単位、184B単位でCBCモードの初期化を行う場合は、実際のAVデータのコーディングの最小単位と一致するため、万一の誤りが発生しても、その伝播の影響を最小限に止めることができるというメリットがある。一方、512B単位でCBCモードの初期化を行う場合は、HDDの情報読み出しの最小単位であると共に、暗号化の単位が大きくより内容の推定が困難になるというメリットがある。同様に、2048B単位でCBCモードの初期化を行う場合は、光ディスクの情報読み出しの最小単位であると共に、暗号化の単位が大きくより内容の推定が困難になるというメリットがある。

【0057】また、184B単位でCBCモードの初期化を行う場合は、暗号化されない領域が8B（すなわち、4バイトのソースパケットヘッダとMPEGのトランスポートストリームの先頭4バイトのヘッダ）あるため、同一のメディアアクセスユニット内で記録されるMPEGのトランスポートストリーム（例えば、暗号化の対象とすべきプログラムと暗号化の対象としないプ

ログラムがマルチプレクスされた状態で記録するような場合）の一部だけ暗号化をするといったことが可能になる。8Bの暗号化されない領域の一部に、後続の184バイトが暗号化されているか否かを識別させるビットを設けることができるからである。

【0058】このとき、それぞれのレコーディングパケット毎の暗号化・非暗号化の区別のために、例えば図2（B）に示したソースパケットヘッダの先頭の予約領域中の1ビットを割り当てて区別してもよいし、トランスポートストリームの先頭の4Bの一部に含まれるMPEGで規定される暗号化の状態を示す2ビットの一部を利用することも可能である。後者の場合、暗号化されていない8ビット中の2ビットの値が「00」のとき後続の184バイトが暗号化されていないことを示し、それ以外で暗号化されていることを示すことができる。

【0059】また、図1のCPU23からシークレットファンクション20に供給する値としては、前記の実施の形態のメディアアクセスユニットナンバーに限定されるものではなく、例えば、メディアアクセスユニットを記録する際の各先頭の論理アドレスを利用した番号を供給するようにしてもよい。

【0060】以上の説明は、記録時の暗号化の動作であるが、再生時はHDDから読み出されたデータを復号化部に入力し、記録時の暗号化と同様にして生成した復号鍵に基づいて復号化することができる。すなわち、CPUから書き込まれた種と再生データ中のメディアアクセスユニットナンバーとからシークレットファンクションFを算出し、このシークレットファンクションFから復号鍵を算出して再生データの復号化をする。復号化された再生データは、メモリに一旦書き込まれ、メモリからレコーディングパケットで読み出し、タイムスタンプとタイムスタンプカウンタの値が一致したときにインタフェースへ再生データを読み出す。

【0061】このように、再生時にはCPUから書き込まれた種と再生データ中のメディアアクセスユニットナンバーとからシークレットファンクションFを算出し、このシークレットファンクションFから復号鍵を算出して再生データの復号化するようにしているため、HDD上に暗号化されて記録されているデータの一部分を飛び飛びで再生する高速再生時には、飛び飛びでアクセスする論理アドレスが予め指定されるので、前記テーブルを参照して、その論理アドレスに対応するメディアアクセスユニットのメディアアクセスユニットナンバーを求め、これを用いて一意に復号のための鍵を迅速に算出することができるため、高速再生を支障なく行うことができる。

【0062】

【発明の効果】以上説明したように、本発明によれば、以下の種々の特長を有するものである。

（1）記録すべき情報を暗号化するための暗号鍵を所定

のデータ量毎に更新することにより、暗号鍵が露見した場合でも、その被害を最小限に止めるようにしたため、ハッカーの氣勢をそぐことができる。

(2) 暗号化単位が短く暗号鍵の個数が多くても、所定のデータ量単位毎に公開鍵暗号で暗号鍵の元となる基数を暗号化するようにしているため、処理の負担を軽減することができる。

(3) 一つの記録媒体上に複数の情報が最小単位毎にマルチプレクスされた状態で記録されるような場合、暗号化をしたい情報のみを選択的に暗号化することができる。

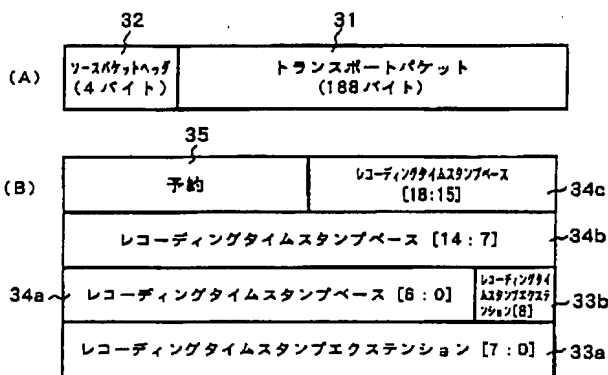
(4) 一つの記録媒体上に複数の情報が最小単位ごとにマルチプレクスされた状態で記録されるような場合（特に、MPEG2のトランスポートストリームのような構造をとって記録される場合）、それぞれの情報の種別を示すIDが暗号化されない部分に含まれると共に、ID毎に適用する情報暗号化用の暗号鍵の系列を異なるものにする事ができる。

(5) 情報を暗号化するための処理が重い場合、すべての情報ではなく選択した一部の要素だけを暗号化しても、特に圧縮された画像データ、音声データのようなものを対象とする場合、意味のある情報の復号や通常の品位での復号を十分不可能とすることができる。

(6) 記録媒体上に暗号化されて記録されているデータの一部分を飛び飛びで再生する高速再生時でも、次にアクセスする所定のデータ量単位の連続番号と論理アドレスの対照表を参照することで、迅速に復号のための鍵を算出することができ、高速再生を支障なく行うことができる。

(7) (6)で参照する値として記録媒体にアクセスする際の論理アドレスを用いると、記録媒体の外部にコピーする場合だけでなく、記録媒体内にも不法なコピーが行われることを排除することができる（論理アドレスは

【図2】



記録媒体内で一意であるため、他の場所にコピーされると復号できなくなる。)

(8) (6)で参照する値として記録媒体にアクセスする際の相対的なポインタを用いると、記録媒体内でどの位置に配置されようと容易に復号することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態の要部のブロック図である。

【図2】図1中のレコーディングパケットの構成とソースパケットヘッダの構成を示す図である。

【図3】ミニマムアクセスユニットの構成の一例を示す図である。

【図4】HDDの場合のミニマムアクセスユニットの構成を示す図である。

【図5】光ディスクの場合のミニマムアクセスユニットの図である。

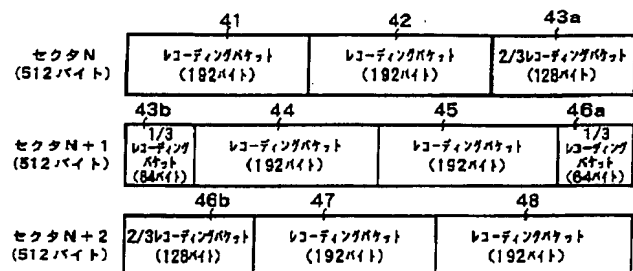
【図6】AVオブジェクトユニットの一例の構成図である。

【図7】メディアアクセスユニットの一例の構成図である。

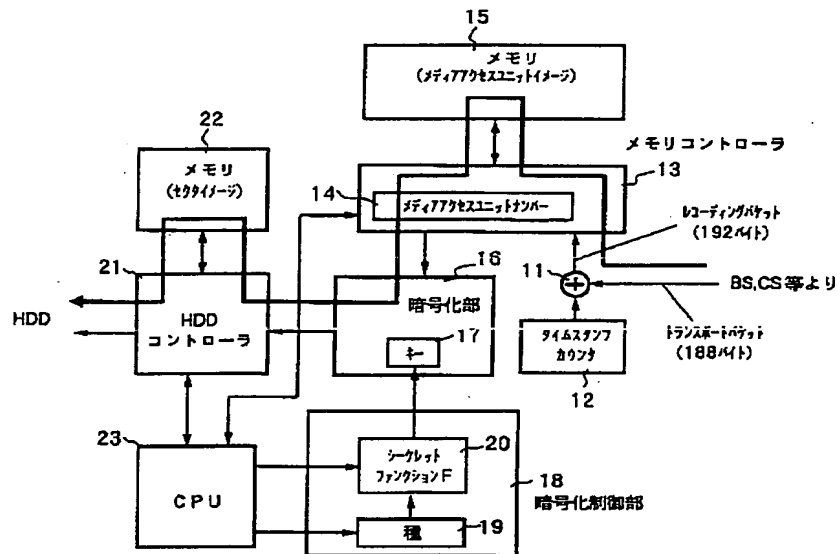
【符号の説明】

- 11 加算器
- 12 タイムスタンプカウンタ
- 13 メモリコントローラ
- 14 メディアアクセスユニットナンバー
- 15、22 メモリ
- 16 暗号化部
- 17 キー（暗号鍵）
- 18 暗号化制御部
- 19 種
- 20 シークレットファンクション
- 21 HDDコントローラ
- 23 中央処理装置（CPU）

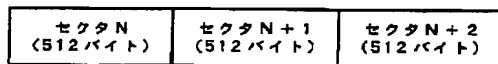
【図3】



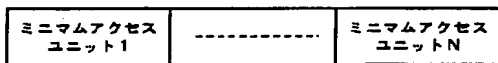
【図 1】



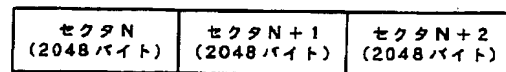
【図 4】



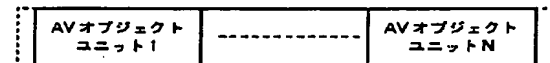
【図 6】



【図 5】



【図 7】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テマコード (参考)

H 0 4 N 5/76

H 0 4 L 9/00

6 4 3

5/91

H 0 4 N 5/91

Z

F ターム (参考) 5B017 AA03 BA07 BA10 CA07 CA16

5C052 AA01 AB02 CC11 DD04

5C053 FA13 GA11 GB21 GB38 LA06

LA07

5D044 AB05 AB07 BC01 CC05 DE12

DE37 DE50 DE83 GK17

5J104 AA00 AA08 AA13 AA41 EA18

JA05 LA02 PA14